UNITED STATES DISTRICT FOR THE
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v.

JOHN STUART,

Defendant.

21-CR-07-LJV-JJM

OBJECTIONS TO REPORT AND RECOMMENDATION; APPEAL OF MAGISTRATE ORDERS

INTRODUCTION

Mr. Stuart previously moved for suppression of evidence seized as a result of a search warrant for the premises at 1010 Cleveland Drive in Cheektowaga, New York, arguing that the information in the warrant purporting to support probable cause was weak and stale. This Court denied that motion.

Since that time, the defense has learned that the scope of the FBI's investigation was much broader than it has let on. In his application in the support of the search warrant, Officer Michael Hockwater, a police officer for the Town of Cheektowaga, claimed to be relaying information from an undisclosed foreign law enforcement agency ("FLA") that an IP address, later learned to be associated with the Cleveland Drive address, had accessed a child pornography website on May 28, 2019. But the defense has learned that this case is merely a small part of a vast multi-district, multi-national pornography investigation. Other exceptionally similar, if not identical, cases have sprung up throughout the county. It has further learned that there is not one but two FLAs at issue, and that the server hosting the website was taken down by authorities in the second country, no mention of which was made in the search warrant affidavit.

Based on the newly discovered information and representations made by counsel about the nature of that information, the defense requested leave to file a motion to compel, while anticipating further motions based on the response (or lack thereof) to the motion to compel. This Court referred the matter to Judge McCarthy for disposition.

Mr. Stuart then filed the aforementioned motion to compel. (Docket No. 55). The government responded to that motion in a fashion that Mr. Stuart has characterized as "too little, too late." In other words, the government's response revealed what the defense had anticipated: that the motion to suppress needs to be reopened and that this Court should order a *Franks* hearing. Mr. Stuart then moved before Magistrate Judge McCarthy to: (1) suppress the evidence located as result of the search warrant for the premises at 1010 Cleveland Drive in Cheektowaga, New York, and (2) order a *Frank's* hearing pursuant to *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). In addition, Mr. Stuart moved to modify a protective order. (Docket No. 85.)

Judge McCarthy recommended that this Court deny the motions for a *Franks* hearing and to suppress. (Report and Recommendation, "R&R"; Docket No. 33.). And he denied the motion to compel and to modify the protective order. Mr. Stuart hereby objects to that recommendation and appeals the denials. For the following reasons, this Court should reject the recommendation and order suppression.

STANDARD OF REVIEW

The standard of review for objections to a Report and Recommendation is *de novo*. The District Court Judge "may accept, reject, or modify the recommendation, receive further evidence or resubmit the matter to the magistrate judge with instructions." *See* FED. R. CRIM. P. 59(b)(3). This standard applies to the objections to the recommendation that this Court deny the motions to suppress and for a *Franks* hearing.

The standard of review for non-dispositive matters – in this case, the motion to compel and the motion to modify the protective order – is not *de novo*. Rather, "[t]he district judge must consider timely objections and modify or set aside any part of the order that is contrary to law or clearly erroneous." FED. R. CRIM. P. 59(a).

ARGUMENT

Motions to Suppress and for a *Franks* Hearing

A. Background

The search warrant application is at the heart of this motion. It provides that:

> In August 2019, a foreign law enforcement agency (referenced herein as "FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that FLA determined that on May 28, 2019, IP address 74.77.4.235 "was used to access online child sexual abuse and exploitation material" via a website that the FLA named and described as the TARGET WEBSITE.
>
> FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

(Search Warrant Application, ¶¶ 24-26, Attached as Ex. A).

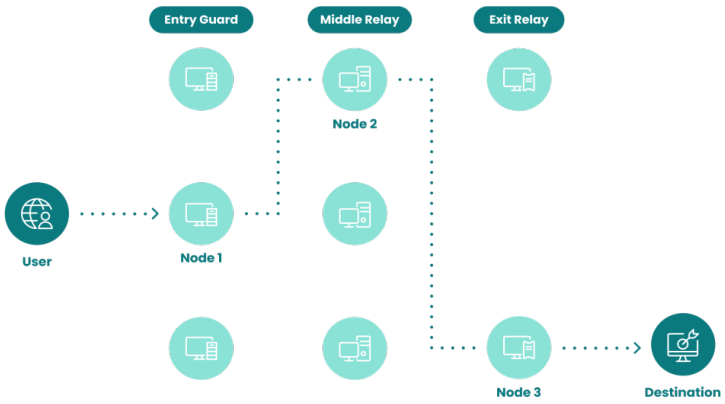
The defense has since learned there is much more to this story. And, in fact, this summary of the investigation is intentionally misleading. In response to the motion to compel, the government composed a letter to the defense to "provide additional information" regarding the background of the investigation that led to the search of Mr. Stuart's home. (Letter attached as Ex. 1 to Reply to Motion to Compel, Docket No. 80, under seal). The government asserts in the letter that the information it contains is "neither discoverable, nor relevant to any material issue" but is provided to "clarify protentional misunderstandings."

The defense disagrees with the characterization that the information provided in the letter, as well as other still outstanding discovery, is neither relevant nor discoverable. To the contrary, since this information pertains to the manner and method in which a search warrant was obtained to search Mr. Stuart's home, it is both deeply relevant and discoverable. In fact, this information should have been previously disclosed not only to the defense, but more importantly to the issuing-magistrate judge at the time of the warrant application.

The government now claims that one foreign law enforcement agency (FLA) seized the server at issue and another FLA deanonymized the IP addresses provided to them by the first FLA.[1] The second FLA, according the government in its letter, "did not disclose to the United States the methodology it used" to uncover the defendant's IP address. None of this was disclosed to the magistrate judge who issued the warrant. In practice, this suggests that by seizing and searching the server (the IP address of which was first identified by the United States government) the first FLA acquired IP address logs of visitors and the second FLA used a yet-to-be identified method to deanonymize the true IP address.

[1] The FLAs at issue are the subject of a protective order but are known to the parties and the Court.

Because the website at issue in this case is hosted by a server on the Tor network, the IP address logs uncovered by the first FLA would be worthless. They would likely represent simply the "exit node" IP address, the last in chain or "onion" of IP addresses that are used to route the request to visit the website. Through this method, Tor can achieve its goal of anonymizing the true user IP's address. To discover where the request to visit a website actually originated, the second FLA would have had to peel back the layers of the onion, or trace the IP addresses through various relay points all the way back to the original user. Below is a graphical illustration of this concept:



Here, the user requests a website identified in the illustration as a "destination." That request is then encrypted and routed through various nodes so that the destination site does not know the original or true user's IP address.

It is this method of unencrypting and tracing back, or unpeeling the union, that the government now claims it is not privy too, and/or does not want to disclose.

But this is the whole ball of wax. Lacking any transparency in this part of the process, it is impossible to know whether whatever method the second FLA used was a reliable and

accurate one. This is especially true given the government's assertion that a NIT[2] was not used. This means that some other new, yet-unknown, potentially untested technique was used. This Court does not know, and the issuing magistrate judge could not have known, the reliability of this technique. To put it bluntly, based on the government latest revelations, there is simply no way to know if the IP address that the second FLA said visited the website *actually visited* the website. The mystery technique might have gotten it wrong. The mystery technique might have identified Mr. Stuart IP's address when it was actually Mr. Smith's, or one of the other millions of IP addresses in the world that visited the site.

Moreover, as the government itself would certainly admit, the prosecutor in this case has no firsthand knowledge of any of the information detailed the letter. It simply represents a hearsay account of an investigation from the government's point of view. Critically, no documents or information have been provided regarding the technique or techniques used to deanonymize the IP addresses that purportedly led to the one associated with Mr. Stuart. Without this crucial information, the government can make no assurance on the reliability or constitutionality of that process. Indeed, there are "two circumstances where evidence obtained in a foreign jurisdiction may be excluded: first, where the conduct of foreign officials in acquiring the evidence is so extreme that it shocks the judicial conscience and second, where cooperation with foreign law enforcement officials may implicate constitutional restrictions." *United States v. Getto*, 729 F.3d 221, 228 (2d Cir. 2013). If the government cannot tell this Court

[2] A NIT or Network Investigation Technique is simply a label the government uses to describe the malware it has installed on American's computers. In the Playpen investigation, for instance the NIT used by the government was malware that was surreptitiously disseminated through a Tor hidden service. The malware was designed to pierce the anonymity provided by the Tor network by placing computer code on users' computers that would transmit private information back to a law enforcement server outside of the Tor network.

how the evidence was gathered, it cannot assure this Court that it does not shock the conscience. Nor can the government assure this Court now, nor the issuing magistrate then, that the process – a process it claims to know nothing about – was a reliable one.

B. A *Frank's* hearing is necessary.

In *Franks v. Delaware*, the Supreme Court held that a defendant is entitled to a hearing to challenge the truthfulness of statements in a search warrant affidavit if he makes "a substantial preliminary showing" that the statements were "knowingly and intentionally [false], or [made] with reckless disregard for the truth," and that the falsehood was "necessary to the finding of probable cause." *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). The right to a *Franks* hearing is triggered not only by false statements but also by material omissions. When a defendant alleges a material omission has been made, the required showing is two-fold: first, the omission must have been either intentional or reckless; and second, the omitted information, if incorporated into the affidavit, must be sufficient to vitiate probable cause. *See, e.g., United States v. Tate*, 524 F.3d 449, 456–57 (4th Cir. 2008) ("A 'literally true' affidavit ... can be intentionally misleading if it deliberately omitted material facts which, when included, would defeat the probable cause showing and thus render false the original 'literally true' affidavit.").

Officer Hockwater made omissions and misstatements knowingly and intentionally, or with reckless disregard for the truth, regarding key issues. First, Officer Hockwater made material misrepresentations about the information he and the FLA had regarding the true nature of the evidence it actually possessed. Second, Officer Hockwater made omissions about the nature, origin, and reliability of the tip from the FLA. Third, Officer Hockwater made

material omissions about the method(s) used by the FLA to identify the IP address. Fourth, Officer Hockwater misrepresented the relationship between U.S. law enforcement and the FLA(s) in the affidavit. Each of these misstatements and misrepresentations went directly to the heart of the probable cause analysis. The magistrate would not have issued the warrant had these misrepresentations been corrected in the affidavit because the reformed affidavit would not establish probable cause.

1. Despite the intended impression of the application, there was no evidence that Mr. Stuart even accessed sexual-abuse material.

Officer Hockwater omitted the crucial fact that the homepage of the website did not display any child sexual abuse material. Screenshots of the website provided by the government show that in order to "access" any child sexual abuse material, an individual would have had to navigate past the homepage of the website. Neither the tip documents nor the affidavit state whether the suspect user IP address did anything beyond accessing the homepage, which contained no contraband images or material. Thus, Officer Hockwater misrepresented the information available to U.S. law enforcement and created a misleading impression that U.S. law enforcement had more evidence of criminal activity than it actually did. Hockwater's misrepresentation about the nature of the tip was recklessly made and was "necessary to the finding of probable cause." *Franks*, 438 U.S. at 155-56. Had Hockwater been truthful about the tip and stated that U.S. law enforcement had received information only that the IP address was used to visit a website where no child pornography was visible or available on the homepage, the magistrate could not have found sufficient probable cause to issue the warrant. Mr. Stuart is therefore entitled to a *Franks* hearing on these false and misleading statements.

Indeed, there is a fundamental difference between: 1) evidence of a one-time visit to a website where no images, videos, or links to child pornography materials were either visible or available on the website's homepage, and no such items were viewed and/or downloaded and 2) evidence of an individual accessing that website and then viewing, downloading, or otherwise possessing materials that would have only been accessible once a user navigated past the homepage. *See United States v. Falso*, 544 F.3d 110, 120-21 (2d Cir. 2008) (finding no probable cause for possession of child pornography when it was alleged that defendant "appear[ed]" to have "gained access or attempted to gain access" to the cpfreedom.com website— which did not require registering an account or logging in—and that even if one inferred that the defendant had accessed cpfreedom.com, there was no specific allegation that the defendant "accessed, viewed or downloaded child pornography"). The information that the FLA relayed to U.S. law enforcement fell squarely into the first category, which, like *Falso*, was insufficient to establish probable cause.

Had Officer Hockwater been truthful about the tip and stated that U.S. law enforcement had received information only that the IP address was used to visit two websites where no child pornography was visible or available on the homepage, the magistrate could not have found sufficient probable cause to issue the warrant. Mr. Stuart is therefore entitled to a *Franks* hearing on these false and misleading statements.

2. There were two FLAs – a fact never disclosed in the warrant application, and there are no assurances in the application about the methods used to acquire the evidence used to apply for the warrant.

In addition to this misrepresentation about the nature of the tip, Officer Hockwater also omitted important information about the origin and reliability (or lack thereof) of the FLA tip.

Specifically, Officer Hockwater stated that FLA (now known to be the second FLA) had "a history of providing reliable, accurate information in the past" and that it was "a national law enforcement agency of a country with an established rule of law." Officer Hockwater averred that the FLA had obtained the information in the tip through an investigation that was "lawfully authorized in the FLA's country pursuant to its national laws," and that the FLA had not "interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain the IP address information." Finally, Hockwater claimed that prior tips from the FLA had led to an arrest, the rescue of children subject to abuse, and the seizure of evidence. However, Officer Hockwater omitted from the affidavit the fact that there was not just one FLA involved in the investigation of the website, but two – from two entirely different countries. The second FLA, which provided the tip to U.S. law enforcement and which Officer Hockwater took pains to assure the magistrate court was subject to the rule of law, was seemingly not involved in the seizure of the website's server. Instead, the government later disclosed (in response to a defense discovery request) that a second FLA seized the server in a country distinct from the tip-giving FLA. Additional information – such as who participated in the seizure and what investigative steps were undertaken by the seizing FLA alone or in conjunction with other countries and/or law enforcement, including the United States – remains unknown. What little *is* known about the second FLA is that it was local to the server host country, which, again, is distinct from the first FLA. Officer Hockwater made no distinction between the two FLAs in the affidavit and failed to inform the court that there was even a second FLA involved in the investigation. Instead, Officer Hockwater created the impression that the tip and the source of that tip both originated from the same, allegedly reliable FLA.

This impression was both misleading and inaccurate. While Officer Hockwater made a number of claims in the affidavit about the reliability of the FLA, those statements applied *only* to the FLA that provided the tip to U.S. law enforcement. There are no facts in the affidavit that address or establish the reliability, trustworthiness, or history of prior tips from the FLA that seized the server. Hockwater did not, for example, make any assurances that the FLA that *seized* the server had a "history of providing reliable, accurate information." Nor did Hockwater aver that the second FLA was from a country with an "established rule of law." Likewise, there are no facts in the affidavit that could have assured the Magistrate that the FLA that seized the server did not conduct a search or seizure of any computer in the United States (e.g., performing a NIT).

This misinformation went to the heart of the probable cause analysis. The tip was the only piece of information that created a nexus between Mr. Stuart, his home, and the alleged criminal activity. Without assurances in the affidavit about the reliability and trustworthiness of the second FLA and the legality of its action, no Magistrate could find there was probable cause.

An expert declaration submitted in a case virtually identical to Mr. Stuart's suggests that the specific IP address could not have been identified without running a NIT – an NIT just like the malware developed by the FBI – or, in the alternative, an error-prone traffic analysis technique. *See* Declaration of Steven Murdoch at ¶ 22-32, *United States v. Sanders*, No. 20-cr-00143 (E.D. Va. Sept. 17, 2021), ECF No. 464-2, attached as Exhibit B. Either scenario would significantly undermine the veracity of the affidavit and its probable cause showing. The deployment of a NIT would constitute an unlawful warrantless search, the results of which could not be considered in Officer Hockwater's affidavit. *See United States v. Tagg*, 886 F.3d 579, 584 (6th Cir. 2018). The use of a NIT would also reveal a substantial misrepresentation in the

affidavit, which relies on Hockwater's assurance that no computer in the United States had been searched. "Malware" is short for "malicious software" which is designed to gain access to or damage a computer without the owner's consent. Malware includes spyware, viruses, and any type of malicious code that infiltrates a computer. In the *Playpen* investigation, for instance, the malware used by the government was surreptitiously disseminated through a Tor hidden service, designed to pierce the anonymity provided by Tor. Thousands of computers, located all over the world, were searched during the *Playpen* investigation in this way.

Alternatively, the fact that the traffic analysis technique described in Professor Murdoch's declaration is inherently error-prone would undermine the strength and reliability of the tip such that no magistrate, had he or she been aware that this technique was used to obtain the IP address, would find there was probable cause.

Judge McCarthy appears to credit the government's argument that Hockwater could not have acted intentionally or deliberately because, as the government argues, Mr. Stuart did not establish or allege that Hockwater was aware of the second FLA's involvement. (R&R, at 18.) But this fundamentally miscomprehends the *Franks* standard. The omission does not have to be deliberate, it can also be reckless. Mr. Stuart had argued, and continues to argue, that it was indeed reckless to take a stock warrant application, drafted by someone else and without any first-hand, personal knowledge of the facts alleged in the application, and present that application to a federal judge as if Hockwater did have such personal knowledge. Indeed, any other result would be make a mockery of the warrant-application process. It would allow federal agents to whitewash all unfavorable facts by conveniently having some other agent present the application to the judge. This head-in-the-sand approach for which the government advocates, and for which the Magistrate Court seems to adopt, cannot be, and is not, the law.

Judge McCarthy goes on to conclude that even if these omission were deliberate, they were immaterial. This is incorrect. If all the tip-passing FLA did was act as a middle-man, which is what the government contends occurred, then that FLA pension for reliability is meaningless. That FLA did not generate the tip and apparently does not know how the seizing FLA came to generate the tip. Adopting this argument puts the Court's imprimatur on the very "tip whitewashing" that was attempted here.

3. The United States was involved years before it received the tip, and was much more than a passive recipient of a tip, as the search warrant avers.

Officer Hockwater's final misrepresentations involved omitting facts about the role of U.S. law enforcement in the investigation. Specifically, Hockwater withheld information that would have shown that 1) U.S. law enforcement was engaged in a "joint venture" with the FLAs and 2) the FLAs engaged in conduct that would shock the judicial conscience such that the FLAs' actions would be subject to the exclusionary rule.

Generally, the Fourth Amendment's exclusionary rule does not apply to foreign searches and seizures." *United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012). There are, however, two exceptions to that rule: "(1) where the conduct of foreign police shocks the judicial conscience, or (2) where American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." *Id*. Here, both exceptions would apply to the conduct of the FLAs. Running a NIT to obtain an IP address of a computer in the U.S. – conduct that is unlawful in the U.S. without first obtaining a warrant – and then hiding that information from a magistrate judge would "shock the judicial conscience." *Id*. Likewise, the information available to the defense suggests that there was a "joint venture" between the United States and the FLAs such that the exclusionary rule would apply to one (or

both) of the FLAs. *See id*. However, Hockwater minimized the collaborative relationship between the agencies and withheld facts that would have established that "American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." *Id*.

The defense's independent investigation and government press releases about the identification and eventual seizure of that server reveal two key pieces of information: (1) years before receiving any "tip" regarding IP addresses from the second FLA in this case, the FBI was significantly involved in the international investigation that led to both the identification and seizure of the server; and (2) finding the server, shutting it down, and de-anonymizing the IP addresses that had visited the website was clearly a joint venture and operation between the U.S. and other countries' law enforcement agencies.

Indeed, the ultimate unearthing of the IP address in this case was the result of an international collaboration beginning sometime in 2017 between INTERPOL, Europol, and law enforcement agencies in the U.S., Austria, France, Italy, the United Kingdom, Australia, Canada, and Brazil.[3] The investigation eventually led to the arrest of a man known by his online moniker "Twinkle" in Portugal. [4] "Twinkle" was an administrator on a child sexual abuse hidden services site called "[website at issue here]," one of five sites operated on the server.[5] In a press release, INTERPOL called the arrest "a textbook example of how

[3] "International collaboration leads to arrest of child sexual abuser in Portugal," INTERPOL (Jan. 23, 2020), https://www.interpol.int/News-and-Events/News/2020/International-collaboration-leads-to-arrest-of-child-sexual-abuser-in-Portugal; Mark Saunokonoko; "Elite Aussie unit helps catch elusive paedophile 'Twinkle' who ran darknet child abuse website'" 9NEWS (Feb. 18, 2020), https://www.9news.com.au/national/queensland-police-taskforce-argos-helps-catch-twinkle-and-babyheart-darknet-site/b5fa55c0-114f-4d66-a66c-045af0bee903. (The Australian Federal Police told *nine.com.au* it helped facilitate the global investigation, which included US, UK, French, Italian, Canadian, Brazilian and Portuguese law enforcement.").
[4] *Id.*
[5] *Id.*

international collaboration can put harmful individuals behind bars."[6]After his arrest, law enforcement was then able to track down another administrator of that site, who lived in Brazil.[7] In 2019 Brazilian authorities found a server that hosted five hidden-services websites focused on the sharing of child sexual abuse materials, including the website at issue here.[8]

The FBI and other U.S. law enforcement agencies were instrumental in the investigation. The FBI's own documentation provides that an investigation was opened as early as January 2017. (Ex. C). Further the FBI helped Brazilian law enforcement locate the IP address of the individual hosting the server.[9] The FBI then used a deanonymization technique to corroborate the identification of the server on the Tor network.[10]

Aided by the U.S.'s investigative techniques, Brazilian authorities were able to determine that the server was ran by Lucas Batista dos Santos, known as "Lubasa."[11] Brazilian law enforcement arrested Lubasa and seized the server in June 2019.[12]

The second FLA itself has said that its investigation was a collaborative effort: "*Working with partners*, the [law enforcement arm of the second FLA] has identified a significant number of unique global internet protocol (IP) addresses on dark web sites; at least 5 percent of these IP addresses are believed to be in the [second FLA country]." (emphasis added).[13]

---

[6] *Id.*
[7] "Operação Lobos," ANPR (Associação Nacional dos Procuradores de Republica (National Association of Public Prosecutors)) (Apr. 18, 2022), available at https://www.anpr.org.br/premiorepublica/votacao-sociedade/conheca-os-finalistas/26336-caso-volkswagen-contribuicao-com-os-orgaos-da-repressao-politica?tmpl=component&print=1. Attached as translated as Exhibit D.
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/an-inspection-of-the-national-crime-agency-criminal-intelligence-function.pdf.

Based on the scant materials made available to the defense by the government and the materials unearthed by the defense, it is clear there was a joint venture between the United States, the two FLAs and other foreign law enforcement agencies to investigate target Tor websites, including the one at issue here. Failing to include the extent to which U.S. law enforcement was engaged in this joint venture to investigate the target websites in Mr. Stuart's case was a significant and material omission. *See United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012); *see also United States v. Mitrovich*, 458 F. Supp. 3d 961 (N.D. Ill. 2020) (finding that the defendant had made a *prima facie* showing, for purposes of motion to compel discovery, that the joint venture doctrine applied and that malware had been used to obtain the defendant's IP address where U.S. law enforcement worked with Australian and New Zealand authorities to uncover IP addresses in the United States).

Further, testimony from the agent in *United States v. Dugan*, which began with a strikingly similar tip from foreign law enforcement, No. 21-cr-00127 (S.D. W. Va. Aug. 2, 2022), again demonstrates that this was indeed a joint venture. When the agent in *Dugan* was put under oath, he testified that U.S. law enforcement "was working jointly with and assisting a foreign law enforcement agency conducting an ongoing investigation." Transcript 61:1-9. Attached as Exhibit E. And he confirmed that foreign law enforcement gave the government the tip as part of that "ongoing investigation." *Id.* at 61:10-62:1. The tip is, therefore, the direct result of a joint venture, which the government hid for years.

At a minimum, a *Frank's* hearing is necessary.

Judge McCarthy again rejected this argument on the basis that there is "nothing to suggest TFO Hockwater was aware of this." (R&R, at 20.) But again, this sanctions the unsanctionable: allowing a federal agent to claim he was unaware of facts that may defeat

probable cause out of reckless ignorance. Hockwater should have been aware: it was his search warrant application!

C. Evidence secured as a result of the search warrant must be suppressed because the complete lack of reliability vitiates probable cause.

This Court should re-open the previously-filed motion to suppress.

The Fourth Amendment prohibits "unreasonable searches and seizures" and requires that "no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the place to be searched, and the persons or things to be seized." U.S. Const., amend. IV; *see also*, Fed. R. Crim. P. 41. Indeed, "[t]he guarantee of protection against unreasonable searches and seizures extends to the innocent and guilty alike. It marks the right of privacy as of the unique values of our civilization and, with few exceptions, stays the hands of the police unless they have a search warrant issued by a magistrate on probable cause..." *McDonald v. United States*, 335 U.S. 451, 454 (1948). For this reason, the judicial approval that a valid warrant confers acts as a checkpoint between the government and its citizens. *Steagald v. United States*, 451 U.S. 204, 212 (1981). An invalid warrant, however, confers nothing of the kind.

It is the government's burden to establish probable cause, *United States v. Delossantos*, 536 F.3d 155, 158 (2d Cir. 2008), which is determined upon consideration of the totality of the circumstances. *Illinois v. Gates*, 462 U.S. 213, 230-232, 238-239 (1983). Because of what's at stake, this includes the issuing court carefully evaluating the reliability of law enforcement's source of information. As the Supreme Court has long recognized:

> The arrest warrant procedure serves to insure that the deliberate, impartial judgment of a judicial officer will be interposed between the citizen and the police, to assess the weight and credibility of

> the information which the complaining officer adduces as probable cause. To hold that an officer may act in his own, unchecked discretion upon information too vague and from too untested a source to permit a judicial officer to accept it as probable cause for an arrest warrant, would subvert this fundamental policy.

Wong Sun v. United States, 371 U.S. 471, 481-482 (1963) (internal citation omitted).

While it is improper to "discount an informant's information *simply because* he [or she] has no proven record of truthfulness or accuracy," *United States v. Canfield*, 212 F.3d 713, 719 (2d Cir. 2000) (emphasis added), the veracity and basis of knowledge of the informant are still "highly relevant" in this determination. *Gates*, 462 U.S. at 230; *see also*, *United States v. Wagner*, 989 F.2d 69, 73 (2d Cir. 1993) (recognizing that a CI's veracity and quality of sources are to be considered in evaluating reliability). If there is ultimately corroboration shown for the informant's claims, his or her entire account may be credited. *Gates*, 462 U.S. at 234-235 (describing a balanced assessment of "all the various indicia of reliability (and unreliability)"); *Canfield*, 212 F.3d at 719-720. Naturally, this Court must consider the "particular factual contexts" of each case. *Gates*, 462 U.S. at 231. The reliability of the information from an informant is examined on a totality of the circumstances standard. *See*, *United States v. Smith*, 9 F.3d 10007, 1012 (2d Cir. 1993), citing *Gates*, 462 U.S. at 230-231.

At bar, the search warrant is significantly dependent on unnamed *foreign* law enforcement agency references, specifically in paragraphs 24 through 27. According to the warrant application, the (now second) FLA is a "national law enforcement agency of a country with an established rule of law." ¶ 26. It is beyond dispute the information this foreign agency has purportedly provided to the FBI is critical to the warrant application.

As the Supreme Court has held, "an officer's statement that affiants have received reliable information from a credible person and believe that heroin is stored in a home, is [] inadequate." *Gates*, 462 U.S. at 239 (internal quotation marks and citations omitted).

Further, as *Gates* makes clear, this principle – that a bare assertion of an informant's claimed credibility and reliability is insufficient – has been established for nearly 40 years. Good faith, then, cannot serve to uphold this deficient warrant. *See, e.g.*, *United States v. Leon*, 468 U.S. 897, 922 (1984). It was at least grossly negligent of the agents to keep this information hidden and ask the magistrate judge to simply affirm the claimed reliability of the informant without even bothering to disclose where the information came from. *See Herring v. United States*, 555 U.S. 135, 144 (2009) ("[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct.").

When an affidavit relies on information provided by a confidential informant, the affidavit must provide some information from which a magistrate can credit the informant's credibility. Here, the affidavit submitted in support of the search warrant failed to establish a "fair probability" that evidence of a crime would be found in Mr. Stuart's home. *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983). The affidavit relied entirely on an unsubstantiated allegation of criminal activity by an unidentified foreign law enforcement agency (now known). The affidavit failed to include any information as to how the second FLA came across that information, how reliable the method the second FLA used to obtain the information was (if indeed it was that FLA that deanonymized the suspect user IP address here), and whether the IP address and/or other tip information was obtained through the second FLA's first-hand knowledge or through other sources.

This Court previous issued a decision, quoted in the most recent Report and

Recommendation, finding that the name of the FLA, or the agency within the FLA is immaterial because that FLA had a track record, at least accordinding to the application, of providing reliable information in the past.

Critically, this Court issued that decision under the intentionally misguided position that there was a single FLA that generated and issued the tip. That was the impression intentionally left by the warrant application, the impression that the defense was under, and even the impression of the prosecuting AUSA was under at the time the first suppression motion was argued before this Court. That fact alone – that no one in the courtroom had but half the facts – should raise this Court's eyebrows.

Since that decision was issued by this Court, the defense learned that a second FLA used an unknown technique to deanonymize the IP addresses. This new information firmly underscores that the blanket assertion in the search warrant application – that the second FLA has provided "accurate and reliable information" in the past – is so broad and vague as to be meaningless. The warrant affidavit does not, and seemingly cannot, make any assurance as to the reliability of the method used to produce the IP address in this case. The affidavit does not even specify whether the FLA's purported previous reliability has anything to do with the subject area at issue in this case. For all we and the issuing magistrate know, the FLA has provided accurate tips about the whereabouts of suspects on the run, or drug dealers' selling habits. This would have no bearing on the issuing-magistrate's confidence in the manner in which the tip in this case was generated, and tellingly no assurances whatsoever on that score are provided.

Moreover, we now know that the FLA did in fact *not* provide accurate and reliable information. The "tip" itself, which was only disclosed after this Court and the District ruled

on the motion to suppress, provides that a certain IP address "was used to access online child sexual abuse and exploitation material." But we now know that the government cannot say whether in fact that is true. All the government can claim to know is that this IP address accessed a website that has as its primary purpose the display of sexual-abuse material. As the government knew at the time but did not make clear to the issuing magistrate judge, there is no evidence that the user behind the IP address ever actually accessed any of this material. Users of the website are met with a webpage that contains absolutely no sexual-abuse material. The only evidence that the government has now, or ever had, is the IP address was used to access this webpage – not that the user or the IP address accessed sexual-abuse material.

We also now know that this assertion did not even come from Hockwater's own personal knowledge, but rather from a stock application that Hockwater simply passed on to the issuing-magistrate judge as a middleman. In other words, the sworn assertion on which this Court based its Report and Recommendation – that the second FLA has provided accurate and reliable information in the past – did not even come from Hockwater himself. Accordingly, this Court should re-open the motion to suppress and suppress the evidence obtained as a result of the search warrant for want of reliability.

Judge McCarthy incorrectly dismisses these arguments without providing rationale, writing simply that they "do not undermine the indicia of reliability." Of course, for the reasons articulated above, Mr. Stuart sees it much differently, and, it is submitted, so should this Court.

Finally, Judge McCarthy finds that, even were he to agree with Mr. Stuart on the merits, good faith would save the day for the government. (R&R, at 22.). This is incorrect for many of the same reasons that this Court should order a Franks hearing and/or suppression.

That is, that the FBI deliberately concealed facts about its investigation to mislead the magistrate into issuing a search warrant. *See, e.g.*, *United States v. Clark*, 638 F. 3d 89, 100 (2d Cir. 2011) (listing, among the circumstances where the good faith does apply, where the issuing magistrate had been knowingly misled.).

Judge McCarthy further appears to conclude that Hockwater's boilerplate statement in his application that he did not include "all" known facts is a sort of panacea that permits omissions. (R&R, at 23) (quoting Hockwater's application for the proposition that he did not include all known facts but only those necessary for probable cause). But of course this cannot cure material omissions. Rather, if the omissions are a result of recklessness and bare on the probable cause determination, then suppression is warranted whether or not the applicant "expressly averred" (R&R, at 23) that he or she was making omissions. *See, e.g., United States v. Lauria*, 70 F.4th 106, 125 (2d Cir. 2023) ("Thus, a defendant seeking to suppress evidence obtained pursuant to an affidavit containing erroneous information must satisfy both a state of mind requirement and a materiality requirement by showing that (1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the issuing judge's probable cause finding.) (internal citations and quotation marks omitted).

***

Motions to Compel and to Modify the Protective Order

This Court should set aside Judge McCarthy's decision to deny the motion to compel and keep in place the overly restrictive and unnecessary protective order.

A. Motion to Compel

While Mr. Stuart continues to assert that he is entitled to documents and information outlined in the motion to compel, if the government's representation is accurate – that is cannot produce documents or data that explain how it acquired the IP address at issue – then, as argued above, this Court must grant the motion to suppress.

B. Motion to Modify the Protective Order

The government bears the burden of establishing good cause to keep discovery and court filings secret, since court proceedings are presumptively open to the public. This investigation that led to this arrest is over. The websites are shutdown. While it may be true that certain information is not "widely known," that is not the standard at issue, and, furthermore, the FBI's joint investigation into this website is certainly widely known in all circles where it matters. It is immaterial that there may be other means for the defense to accomplish its objectives absent a modification of the protective order. First, the means identified by the government and the magistrate court are cumbersome and raise their own issues. Second, that again is not the standard. The government must show, not simply allege, that the protective order is necessary. It cannot do that here.

CONCLUSION

This Court should suppress all the evidence obtained as a result of the search warrant, or order a *Franks* hearing based on the omissions and misrepresentations contained in the Hockwater application.

Dated: Buffalo, New York
August 7, 2023

Respectfully submitted,

/s/ Jeffrey T. Bagley
Jeffrey T. Bagley
jeffrey_bagley@fd.org
Assistant Federal Public Defenders
Federal Public Defender's Office
300 Pearl Street, Suite 200
Buffalo, New York 14202
(716) 551-3341
Counsel for John Stuart